Centralized Data Collection and Integration System (CDCIS) PIA

1. Contact Information

A/GIS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of system: Centralized Data Collection and Integration System

(b) Bureau: A/EX

(c) System acronym: CDCIS

(d) iMatrix Asset ID Number: 255433

(e) Reason for performing PIA: Click here to enter text.

☒ New system

☐ Significant modification to an existing system

☐ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
Under Review

(c) Describe the purpose of the system:
The Centralized Data Collection and Integration System (CDCIS) is a new system that will be an on-premise instance of ServiceNow operating on OpenNet. The software will replace the Visual eForms, legacy forms solution using Cerenade, which hosts more than 600 government forms.

The ServiceNow (version Helsinki) software will be used to support information collection and business processes for timely, secure, and accurate submission of government forms.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
CDCIS will collect the data that individual users input into the user profile and various forms. There are certain forms that request PII needed for business purposes. These forms include a Privacy Act Statement. The kinds of PII collected by these forms may include Names, Birthdates, Financial Account Numbers, SSN, Phone number(s), Business Addresses, Personal Address, e-mail addresses, images or biometrics IDs and medical information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
Each form is owned by a bureau/office; not owned by DIR. The form owner from the respective bureau/office designs the form to collect the information needed. If the bureau/office wants to collect PII in a form, they are required to include a Privacy Act statement outlining the appropriate authority and DIR refers them to the Privacy Office for approval. Example legal authorities and/or agreements include:

- 22 U.S.C. 4081, Travel and Related Expenses;
- 5 U.S.C. 301, 302, Management of the Department of State;
- 22 U.S.C. 2581, General Authority;
- 22 U.S.C. 3921, Management of the Foreign Service;
- 22 U.S.C. 3927, Responsibility of Chief of Mission.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide: The purpose of CDCIS information collection and method of record accessibility is addressed by the published SORNs listed below.

- SORN Name and Number: State-31 (Human Resources Records), State-36 (Security Records), State-56 (Network User Account Records), and OPM/GOV'T-1 (General Personnel Records)
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 19, 2013; December 15, 2015; October 14, 2010; December 11, 2012

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .) A/EX is coordinating the records retention schedule with the Records Office.

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): see table below
- Length of time the information is retained in the system: see table below
- Type of information retained in the system:
  see table below:

Record Type	Schedule No.	Length of Retention (time)	Information Type
Forms Control Files	DispAuthNo: New Item (Supersedes NC-59-75-14, item lOa)	Temporary. Destroy/delete active docket material with prior revisions when 7 years old or when discontinued, whichever is sooner.	Background docket materials, requisitions, specifications, processing data, control records and the forms. Files in electronic format as of January 1,2011.
Forms Files	DispAuthNo: GRS 16, item 3a	Temporary. Cutoff and retain files in NGIS/DIR after related form is discontinued, superseded, or cancelled. Destroy/delete 5 years after form is discontinued, superseded, or cancelled.	Department of State centralized active/discontinued form files containing the request for form creation (DS-1855), any requests for form revisions, email or written correspondence, form design notes, approval to publish and approval to discontinue. Maintained in hard copy/electronic format from start-up through December 31, 2010. Files provided in electronic format as of January 1,2011.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees

☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?
Each form is owned by a bureau/office; not owned by A/GIS/DIR. The bureau/office form owner designs the form to collect the information desired. If they want to collect SSN, they are required to include a Privacy Act statement stating a programmatic specific authority permitting the collection of SSN. The authorizing statement is displayed on the respective form(s).

(c) How is the information collected?
Information is provided by Department users when they save a form as a draft or submit a form. The information is saved in a mySQL database.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.
Click here to enter text.

(e) What process is used to determine if the information is accurate?
Each CDCIS user is responsible for ensuring their data is accurate on their user profile and in forms they submit. Relevant validation rules will also be included in select forms.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Each CDCIS user is responsible for ensuring their data is accurate on their user profile and in forms they submit. For applicable forms, an Approver may manually review information and request updates to submitted information via the system workflow.

(g) Does the system use information from commercial sources? Is the information publicly available?
No

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes. Individuals are notified about collection of their information through text instructions at the point of data submission and relevant Privacy Act provisions where applicable. Individuals may access their information through CDCIS at any time after submission.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
Users grant consent by logging into the CDCIS application and submitting a form that contains PII that they have entered.

- If no, why are individuals not allowed to provide consent?
Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?
Personal data is collected only when required by business processes. Users are notified of the specific requirements with the respective Privacy Act text. The minimum amount of personal data required to support requests is included in a user profile (Name, Business E-Mail, Address, and Phone Number). Additional personal fields only appear on forms which require that information for completion of the business process. SSN is only requested when needed and, if possible, only the last four digits are collected. The user profile also collects Job Title, Address (Region/Location), Office / Agency, Supervisor, and Time Keeper.

5. Use of information

(a) What is/are the intended use(s) for the information?
Information is used to fulfill various business processes across the Department such as requesting a new user account, obtaining approval to take leave, receiving a badge, or requesting petty cash. Fulfillment of these processes commonly requires the name and contact information (name, e-mail address, phone number).

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes, information is solely used for requesting and fulfilling information collection as requested by the bureau/office who designed the data collection instrument.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?
CDCIS software (ServiceNow) includes out-of-the box reporting functionality to report on key metrics about forms submitted, such as the number of a particular form that has been submitted. The Department currently collects the same information, but rarely analyzes information stored in the system as analysis requires custom reports generated through a web service integrated with Cerenade.

(2) Does the analysis result in new information?
No

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?
☐Yes ☒No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Information stored in the system database is only available to the system administrators. Information collected through an instrument designed by Bureaus/offices for the purpose of data collection will be shared accordingly. Bureaus/offices will not be able to access information collected in instruments owned by another bureau/office during the initial system rollout. There is potential for data sharing and integration in future releases, at which point the PIA will be updated accordingly.

(b) What information will be shared?
Information will not be shared across bureaus/offices. Information could be shared with Supervisors designated with the Approver role by a user. The person submitting the form will control with whom their information is shared when they identify Supervisors or Approvers in their user profile.

(c) What is the purpose for sharing the information?
Information is shared to allow for the fulfillment of the requested business process.

(d) The information to be shared is transmitted or disclosed by what methods?
Information is shared via workflow functionality which routes a request through necessary steps in the fulfillment process. This workflow may vary based on request type.

(e) What safeguards are in place for each internal or external sharing arrangement?
Supervisors and Approvers are assigned by the user in the user profile. The ISSO monitors the system administrator’s access. Any additional information sharing is arranged by the bureau/office that owns the form.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
Privacy concerns surrounding access to PII are addressed by including those fields only on forms where the information is needed for business purposes. DIR refers bureaus/offices requesting the form to the Privacy Office to confirm nature of information being collected.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Users are able to view and update their personal information on their user profile and look up any forms they have submitted in the system.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

Users are able to update their personal information on their user profile. Users may update information within a form at any point before it is completed. Thereafter, users must submit a new form to provide additional information.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Each form contains instructions about the submission of information. A user may change information or save in-progress drafts, but cannot change information once a form is completed through the workflow process. To correct information in a form that has been completed, users would need to submit a second form.

8. Security Controls

(a) How is the information in the system secured?

Access to CDCIS is enabled through Single Sign-On on OpenNet and is accessed over a secure HTTPS connection. Users only have the ability to submit forms and view forms that the individual has already submitted. An individual may also indicate a Supervisor or Approver who has access to relevant submitted forms.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Information will be available to the individuals who originally submitted the form. If supervisor approval is needed to complete the business process request, CDCIS users will indicate the appropriate Approver when they submit the form. Approvers only have access to view information submitted by users who designate them as a Supervisor in the user profile.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Actions taken within CDCIS are logged and viewable by the system administrator. The assigned Information System Security Officer (ISSO) and Application Information System Security Officer (AISO) are responsible for monitoring and auditing the system. Audit logs will be viewed as required by the Department’s security rules and regulations.

(d) Explain the privacy training provided to authorized users of the system.

The Department of State authorized users have taken mandatory FSI courses PS800 Cyber Security Awareness, annually and PA459 Protecting Personally Identifiable Information at least within the first 90 days of employment.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
The Department provides "single sign on" whereby once a user signs on to his/her computer using a User ID and password, the user is automatically authenticated to access applications (like CDCIS) that exist on the Department's network.

All data within CDCIS is encrypted with FIPS 140-2 compliant algorithms at the database and application level. In addition, FAM compliant password complexity is in place for authentication within the system.

(f) How were the security measures above influenced by the type of information collected?
Security measures were put in place specifically to meet FISMA Moderate and FedRAMP Moderate requirements. The vast majority of data collected is unclassified and not sensitive.

9. Data Access

(a) Who has access to data in the system?
Department of State employees will have access to their own data and, if applicable, any data submitted to them in their supervisor/approver capacity through OpenNet.

(b) How is access to data in the system determined?
Access to data is determined by the individual user and role.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
OpenNet users only have access to their own data or data submitted to them. Access to data in CDCIS is restricted based on roles assigned to an individual's User ID.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Users can only see forms that they are authorized to browse based on the roles assigned to their user profiles.

Both the assigned Information System Security Officer (ISSO) and Application Information System Security Officer (AISO) are responsible for monitoring and auditing the system. In addition, users receive training in Privacy Awareness, Privacy Act, and the mandatory Annual Cyber Security Awareness course and exam.